

UNITED STATES PATENT APPLICATION

for

A SECURE NETWORK OUTLET FOR SUPPORTING IP DEVICE ADDRESS
ASSIGNING FUNCTIONALITY

Inventors:

Alan Rubinstein
Gary Wang
Yung-Fu Chang

prepared by:

WAGNER, MURABITO & HAO LLP

Two North Market Street

Third Floor

San Jose, CA 95113

(408) 938-9060

SECURE NETWORK OUTLET FOR SUPPORTING IP DEVICE ADDRESS
ASSIGNING FUNCTIONALITY

RELATED U.S. APPLICATIONS

5 This application claims priority to the copending provisional patent applications: patent application serial number 60/277,593, attorney docket number 3COM-3650.BCG.US.PRO, entitled "'Intellijack' physical concepts," with filing date March 20, 2001, and assigned to the assignee of the present invention; patent application serial number 60/277,767, attorney docket number 10 3COM-3651.BCG.US.PRO, entitled "A method for managing intelligent hardware for access to voice and data networks," with filing date March 20, 2001, and assigned to the assignee of the present invention; patent application serial number 60/277,451, attorney docket number 3COM-3652.BCG.US.PRO, entitled "A method for filtering access to voice and data networks by use of 15 intelligent hardware," with filing date March 20, 2001, and assigned to the assignee of the present invention; patent application serial number 60/277,592, attorney docket number 3COM-3653.BCG.US.PRO, "'Intellijack' usage," with filing date March 20, 2001, and assigned to the assignee of the present invention; and patent application serial number 60/285,419, attorney 20 docket number 3COM-3722.BCG.US.PRO, "Intelligent concentrator," with filing date April 20, 2001, and assigned to the assignee of the present invention.

FIELD OF INVENTION

The present invention relates to the field of computer networks. In particular, the present invention relates to secure network outlet for supporting internet protocol (IP) device address assigning functionality in an intelligent data concentrator.

BACKGROUND OF THE INVENTION

As computer networks increasingly proliferate in society, the number of devices coupled to computer networks grows at a fast rate. Traditionally, one cable connects a single RJ-45 port of the outlet to a local area network (LAN) wiring closet and multiple ports requires additional wiring. A network outlet, such as a switch or a hub, connects multiple network devices to LAN port located in a wiring closet.

Additional cables are needed for multiple ports on the network outlet, thereby increasing the network layout and cabling while limiting network accessibility. As one cable is required to connect each computer to the LAN port of the wiring closet, the costs associated with connecting more computers to the LAN are very high, particularly in wiring and installation costs.

Additionally, each computer requires a unique global IP address assigned to the outlet. As such, a large number of global IP addresses are consumed.

One limitation with regards to computer networks is that there are only a limited number of global IP addresses. As it is becoming more necessary to connect more computers to LANs and the Internet, the number of global IP addresses being consumed is increasing, thus decreasing the available number of global IP addresses. Implementing Network Address Translation (NAT) technology in a network outlet is useful in saving the consumption of the global routable IP addresses within a LAN. Under NAT, one global IP address is assigned to the outlet for connection to the LAN while private IP addresses are used to control multiple devices within the personal area network (PAN).

One drawback to the use of network outlets, such as a stand-alone switch or a firewall device, is that they are subject to misuse or theft. Network outlets are typically unmanaged and do not have built-in access control. In particular, network outlets are typically not secure. Furthermore, network outlets implementing firewall/security policies are not centrally managed or distributed by a trusted source.

Accordingly, a need exists for a secure network outlet for coupling an electronic device to a network. A need also exists for a method and a device thereof which satisfies the above need for supporting IP device address assigning functionality. A need also exists for a method and device thereof which satisfies the above needs and which reduces the consumption of available global IP addresses within a network. A need also exists for a

method and device thereof that satisfies the above needs and also protects PAN devices by hiding their IP addresses from the external network.

3COM-3720.BCG.US.P/JPW/MJB

SUMMARY OF THE INVENTION

The present invention provides a secure network outlet for coupling an electronic device to a network. The present invention also provides a method and a device for supporting IP device address assigning functionality. The present invention also provides a method and device that reduces the consumption of available global IP addresses within a network. The present invention also provides a method and device that protects PAN devices by hiding their IP addresses from the external network.

10 In one embodiment, the present invention provides a method for performing device address assigning functionality in intelligent hardware. A network access request is received from an electronic device communicatively coupled to the intelligent hardware. In one embodiment, a device address request is transmitted to a network server. A first device address is received at the intelligent hardware from the network server. The intelligent hardware then assigns a second device address to the electronic device.

20 In another embodiment, the intelligent hardware has a pre-assigned first device address and assigns a second device address to the electronic device, such that the intelligent hardware eliminates the need for a separate device address assigning server. The present invention reduces the consumption of global device addresses within a network, and also provides protection to electronic devices by hiding their device addresses from the external network.

In one embodiment, the present invention comprises a first interface for communicatively coupling the intelligent hardware to the network and a second interface for communicatively coupling the intelligent device to a plurality of client devices. The intelligent device also comprises a processor coupled to the first interface. In one embodiment, the intelligent device also comprises a device address retriever for retrieving a device address from a network server and assigning a device address to a connected electronic device. In another embodiment, the intelligent device also comprises a device address assignor for assigning a device address to a connected electronic device, such that the intelligent device eliminates the need for a separate device address assigning server (e.g., network server).

These and other objects and advantages of the present invention will become obvious to those of ordinary skill in the art after having read the following detailed description of the preferred embodiments which are illustrated in the various drawing figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and form a part of this specification, illustrate embodiments of the invention and, together with
5 the description, serve to explain the principles of the invention:

FIGURE 1 illustrates an exemplary wired desktop cluster coupled to a local area network (LAN) in accordance with one embodiment of the present invention.

FIGURE 2 is a block diagram of a cross-sectional view of an intelligent data concentrator in accordance with one embodiment of the present invention.

FIGURE 3 is an illustration of a perspective view of an exemplary
15 faceplate of an intelligent data concentrator in accordance with one embodiment of the present invention.

FIGURE 4 is a block diagram of an exemplary network upon which
20 embodiments of the present invention may be practiced.

FIGURE 5 is a flowchart diagram of the steps in a process for performing device address assigning functionality in intelligent hardware (e.g.,

an intelligent data concentrator) having a device address retriever in accordance with one embodiment of the present invention.

FIGURE 6 is a flowchart diagram of the steps in a process for

- 5 performing device address assigning functionality in intelligent hardware (e.g., an intelligent data concentrator) having a device address assignor in accordance with one embodiment of the present invention.

FIGURE 7 is a block diagram of an intelligent data concentrator having a
10 device address retriever configured for performing device address assigning functionality in accordance with an embodiment of the present invention.

- FIGURE 8 is a block diagram of an intelligent data concentrator having a device address assignor configured for performing device address assigning
15 functionality in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION

In the following detailed description, for purposes of explanation, numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will be apparent to one skilled in the art that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are not described in detail in order to avoid obscuring aspects of the present invention.

Some portions of the detailed descriptions which follow are presented in terms of procedures, steps, logic blocks, processing, and other symbolic representations of operations on data bits within a computer memory. These descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. A procedure, computer executed step, logic block, process, etc., is here and generally conceived to be a self-consistent sequence of steps of instructions leading to a desired result. The steps are those requiring physical manipulations of data representing physical quantities to achieve tangible and useful results. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers or the like.

It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussions, it is appreciated that

5 throughout the present invention, discussions utilizing terms such as "receiving", "transmitting", "assigning", "performing", "providing" or the like, refer to the actions and processes of a computer system, or similar electronic computing device, such as intelligent hardware or an intelligent data concentrator. The computer system or similar electronic device manipulates

10 and transforms data represented as electronic quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission, or

15 display devices.

Portions of the present invention are comprised of computer-readable and computer executable instructions which reside, for example, in computer-usable media of a computer system or intelligent hardware (e.g., an intelligent

20 data concentrator). It is appreciated that the present invention can operate within a number of different computer systems including general purpose computer systems, embedded computer systems, and stand alone computer systems specially adapted for controlling automatic test equipment.

The present invention provides a secure network outlet for supporting IP device address assigning functionality. Specifically, the present invention provides intelligent hardware (e.g., an intelligent data concentrator) for

5 assigning a device address to an electronic device communicatively coupled to the intelligent hardware. In one embodiment, the intelligent hardware can operate as either a device address retriever for communicating with a network server for assigning a device address. In another embodiment, the intelligent hardware operates as a network server for assigning a device address, such

10 that the intelligent hardware eliminates the need for a separate device address assigning server.

Figure 1 illustrates an exemplary personal area network (PAN) 100 coupled to a local area network (LAN) 150 in accordance with one embodiment of the present invention. PAN 100 comprises IP telephony 110, notebook 120, desktop workstation 130, and printer 140, each of which is communicatively

15 coupled to intelligent data concentrator 210. Intelligent data concentrator 210 is coupled to LAN 150, thus acting as an interface from the various client devices (e.g., comprises IP telephony 110, notebook 120, desktop workstation 130, and

20 printer 140) to LAN 150.

In one embodiment, the electronic devices of PAN 100 (e.g., comprises IP telephony 110, notebook 120, desktop workstation 130, and printer 140)

receive power over LAN 150 through intelligent data concentrator 210. In the present embodiment, a remote power source transmits power across LAN 150 to intelligent data concentrator 210. Electronic devices coupled to intelligent data concentrator 210 may be configured to receive power over LAN 150.

5

Figure 2 is a block diagram 200 of a cross-sectional view of an intelligent data concentrator 210 in accordance with one embodiment of the present invention. This embodiment of the present invention implements intelligent hardware that is easy to install and reliably provides an attachment point for access to voice and data networks 240. The embodiment is implemented through miniaturized hardware that can be installed inside of a wall or in internal space provided for in an office cubicle. One surface 230 of this embodiment is intended to be accessible by the end user and would in most instances be on an external surface of a workspace.

10

15

A plurality of ports 220 are mounted on the external surface 230 of this embodiment. In one embodiment, communication port 220 is an RJ-45 jack. In another embodiment, port 220 is an RJ-11 jack. It should be appreciated that port 220 is not limited to any particular jack, and that any type of communication port can be used. Additionally, while intelligent data concentrator 210 illustrates four ports 220, it should be appreciated that alternative implementations could support a greater or lesser number of ports 220.

20

Connections to the central data (LAN) or voice network 240 are terminated at intelligent data concentrator 210 for coupling to ports 220.

Termination of the network cabling 250 (voice or data) will provide for both a reliable electrical and mechanical connection for industry standard communications cabling such as CAT-3, CAT-5, CAT-5E or similar cabling.

In one embodiment, intelligent data concentrator 210 assigns a device address to electronic devices connected through ports 220 for communicating over network 240. Intelligent data concentrator 240 communicates with remote network server 260 for assigning device addresses to connected electronic devices. In one embodiment, intelligent data concentrator 210 operates as a device address retriever for communicating with network server 260 for assigning a device address.

In one embodiment, mounting hardware attaching intelligent data concentrator 210 to the wall also comprises a tamper detection means 270. In one embodiment, tamper detection means 270 is tamper detection hardware or a tamper detection switch. If a user attempts to circumvent the security measures by physically removing intelligent data concentrator 210, the act of removing the mounting screws would be detected by tamper detection means 270 and an alerting message would be transmitted to a central control site over network 240. In one embodiment, the attempt would be logged and a control

message could be sent to a centralized management station that could disallow network traffic on the segment that intelligent data concentrator 210 was attached to.

5 Figure 3 is an illustration of a perspective view 300 of an exemplary user-accessible surface 230 of an intelligent data concentrator 210 in accordance with one embodiment of the present invention. A user is able to connect data devices to a voice or data network through ports 220. As described above, in one embodiment of the present invention, intelligent data concentrator 210 is
10 configured to transmit power to connected electronic devices through ports 220.

 Figure 4 is a block diagram of an exemplary LAN 400 upon which embodiments of the present invention may be practiced. In one embodiment,
15 LAN 400 comprises network server 405 and intelligent hardware 410, 415, and 420. In one embodiment, intelligent hardware 410, 415 and 420 are intelligent data concentrators (e.g., intelligent data concentrator 210 of Figure 2, intelligent data concentrator 702 of Figure 7 or intelligent data concentrator 802 of Figure 8). In one embodiment, network server 405 is used for retrieving and
20 assigning a device address to an electronic device communicatively coupled to intelligent hardware 410, 415 and 420. 420 are communicatively coupled to network server 405 over links 440, 445 and 450, respectively. In one embodiment, links 440, 445 and 450 are network cabling. In one embodiment,

links 440, 445 and 450 also are coupled a power source (e.g. power source 250 of Figure 2 or power source 609 of Figure 6), such that they provide power to intelligent hardware 410, 415 and 420.

5 In one embodiment, intelligent hardware 410, 415 and 420 are connected to network server 405 by means of network cabling. In the current embodiment, CAT 3 or 5 cabling is used and an Ethernet physical interface is employed. However, it should be appreciated that the present invention will work with other types of LANs, such as LANs with differing physical
10 connections or adopted for use in RF wireless and optical systems. As discussed above, in one embodiment, links 440, 445 and 450 also provide power to intelligent hardware 410, 415 and 420. In one embodiment, the power is supplied over network cabling.

15 Intelligent hardware 410 is coupled to electronic devices 425a and 425b. Similarly, intelligent hardware 415 is coupled to electronic devices 430a, 430b and 430c, and intelligent hardware 420 is coupled to electronic devices 435a and 435b. It should be appreciated that electronic devices can comprise any number of data devices or client devices, including but not limited to: computer
20 systems, printers, voice IP telephones, and fax machines configured for use over voice IP networks.

In one embodiment, the intelligent hardware is configured to provide power to connected electronic devices. For example, in the present embodiment, intelligent hardware 410 supplies power to electronic devices 425a and 425b. It should be appreciated that electronic devices connected to an intelligent hardware may receive power over LAN 400. Power is supplied to the intelligent hardware, and an electronic device configured to receive power through the intelligent hardware receives its operating power through the intelligent hardware.

Figure 5 is a flowchart diagram of the steps in a process 500 for performing device address assigning functionality in intelligent hardware (e.g., intelligent data concentrator 702 of Figure 7) having a device address retriever in accordance with one embodiment of the present invention. Steps of process 500, in the present embodiment, may be implemented with any computer languages used by those of ordinary skill in the art.

At step 510 of process 500, the intelligent hardware having a device address retriever receives a network access request from a connected electronic device. It should be appreciated that a network access request is intended to include any request for data over a network. In one embodiment, the network access request is a request to communicate with a computer system located on a corporate network. In another embodiment, the network

access request is a request to communicate with a computer system located on the Internet.

At step 520, the intelligent hardware transmits a device address request to a network server. It should be appreciated that in order for an electronic device to communicate over a network, it requires a device address. The device address operates to ensure that data packets are sent to the correct electronic device. In one embodiment, the device address is an Internet Protocol (IP) address. In one embodiment, the network server is a Dynamic Host Configuration Protocol (DHCP) server.

At step 530, the intelligent hardware receives a device address (e.g., and IP address) from the network server. In one embodiment, the device address is a global IP address.

At step 540, the intelligent hardware assigns a device address to the electronic device. In one embodiment, the intelligent hardware assigns the device address received from the network server to the electronic device. In another embodiment, the intelligent hardware assigns the electronic device a private device address. In one embodiment, the private device address is a private IP address. The present embodiment protects electronic devices connected to the intelligent hardware by hiding their IP addresses from the external network.

Figure 6 is a flowchart diagram of the steps in a process 600 for performing device address assigning functionality in intelligent hardware (e.g., intelligent data concentrator 802 of Figure 8) having a device address assignor in accordance with one embodiment of the present invention. Steps of process 600, in the present embodiment, may be implemented with any computer languages used by those of ordinary skill in the art.

At step 610 of process 600, the intelligent hardware having a device address assignor receives a network access request from a connected electronic device. It should be appreciated that a network access request is intended to include any request for data over a network. In one embodiment, the network access request is a request to communicate with a computer system located on a corporate network. In another embodiment, the network access request is a request to communicate with a computer system located on the Internet.

At step 620, the intelligent hardware assigns a device address to the electronic device, such that said intelligent hardware eliminates the need for a separate device address assigning server. In the present embodiment, the device address assignor operates as a device address assigning server. In one embodiment, the device address assignor operates as a DHCP server.

In one embodiment, the intelligent hardware assigns the electronic device a public device address. In another embodiment, the intelligent hardware assigns the electronic device a private device address. In one embodiment, the private device address is a private IP address. The present
5 embodiment protects electronic devices connected to the intelligent hardware by hiding their IP addresses from the external network. In one embodiment, the intelligent hardware has a preassigned device address.

Figure 7 is a block diagram 700 of an intelligent data concentrator 702
10 having a device address retriever 716 configured for performing device address assigning functionality in accordance with an embodiment of the present invention. In one embodiment, intelligent data concentrator 702 is configured to perform a process for performing device address assigning functionality as described above in process 500 of Figure 5.

15 Intelligent data concentrator 702 comprises a first interface 704 for communicatively coupling intelligent data concentrator 702 to network 708. Intelligent data concentrator 702 also comprises a plurality of second interfaces 706a-d for communicatively coupling intelligent data concentrator
20 702 to a plurality of electronic devices 710a-d. In one embodiment, second interfaces 706a-d are communication ports (e.g., communication ports 220 of Figure 2). It should be appreciated that there can be any number of second interfaces 706a-d, and that the present invention is not meant to limit the

number of second interfaces 706a-d. First interface 704 operating in conjunction with second interfaces 706a-d operates to connect electronic devices 710a-d to network 708.

5 Intelligent data concentrator 702 also comprises intelligence 712. In one embodiment, intelligence 712 comprises processor 714 coupled to the first interface 704 and status device address retriever 716 coupled to the means for processing and interpreting data 714. In one embodiment, processor 714 is a robust processor. In another embodiment, processor 714
10 is a central processing unit (CPU).

 In one embodiment, device address retriever 716 is a software implementation in intelligent data concentrator 702. Alternatively, device address retriever 716 can be implemented by hardware or firmware (e.g., a
15 software or firmware device address retriever).

 In one embodiment, device address retriever 716 operates to obtain a device address for electronic devices connected to intelligent data concentrator 702 through second interfaces 706a-d by communicating with network server
20 709. In one embodiment, network server 709 is a DHCP server. In one embodiment, the device addresses are IP addresses.

Figure 8 is a block diagram 800 of an intelligent data concentrator 802 having a device address assignor 816 configured for performing device address assigning functionality in accordance with an embodiment of the present invention. In one embodiment, intelligent data concentrator 802 is
5 configured to perform a process for performing device address assigning functionality as described above in process 600 of Figure 6.

Intelligent data concentrator 802 comprises a first interface 804 for communicatively coupling intelligent data concentrator 802 to network 808.
10 Intelligent data concentrator 802 also comprises a plurality of second interfaces 806a-d for communicatively coupling intelligent data concentrator 802 to a plurality of electronic devices 810a-d. In one embodiment, second interfaces 806a-d are communication ports (e.g., communication ports 220 of Figure 2). It should be appreciated that there can be any number of second
15 interfaces 806a-d, and that the present invention is not meant to limit the number of second interfaces 806a-d. First interface 804 operating in conjunction with second interfaces 806a-d operates to connect electronic devices 810a-d to network 808.

20 Intelligent data concentrator 802 also comprises intelligence 812. In one embodiment, intelligence 812 comprises processor 814 coupled to the first interface 804 and device address assignor 816 coupled to the means for processing and interpreting data 814. In one embodiment, processor 814 is a

robust processor. In another embodiment, processor 814 is a central processing unit (CPU).

In one embodiment, device address assignor 816 is a software implementation in intelligent data concentrator 802. Alternatively, device address assignor 816 can be implemented by hardware or firmware (e.g., a software or firmware device address assignor). In one embodiment, device address assignor 816 is a DHCP server.

In one embodiment, device address assignor 816 operates to assign a device address for electronic devices connected to intelligent data concentrator 802 through second interfaces 806a-d without requiring a separate device assigning server. In one embodiment, the device addresses are IP addresses. In one embodiment, intelligent data concentrator 802 has a pre-assigned device address.

The preferred embodiment of the present invention, a secure network outlet for supporting IP device address assigning functionality, is thus described. While the present invention has been described in particular embodiments, it should be appreciated that the present invention should not be construed as limited by such embodiments, but rather construed according to the below claims.